New Mexico K-12 Cyber Security Awareness

Strategic Plan 2020 - 2021

Table of Contents

Executive Summary

"The advent of networked technology has spurred innovation, cultivated knowledge, encouraged free expression, and increased the Nation's economic prosperity. However, the same infrastructure that enables these benefits is vulnerable to malicious activity, malfunction, human error, and acts of nature, placing the Nation and its people at risk. Cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure located in the United States and abroad." Presidential Policy Directive/PPD-41.

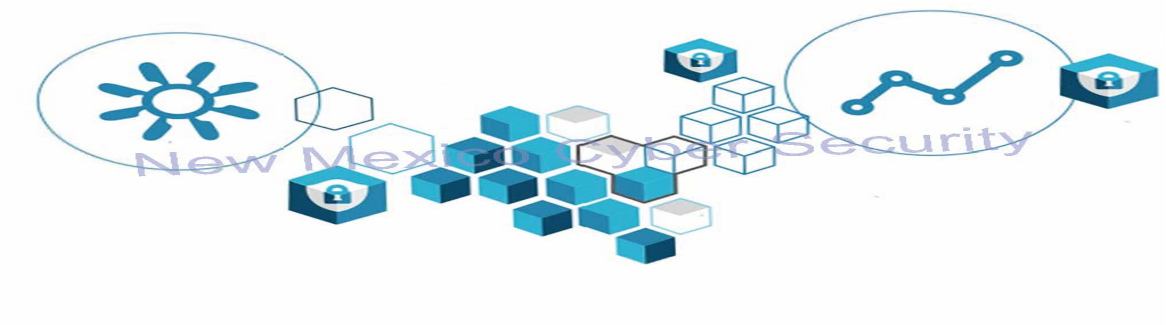
Malicious cyber activities are conducted for a variety of reasons including: financial gain, information/intellectual property theft, activist causes, to disable computer systems or to disrupt critical infrastructure and vital resources of a government or organization.

To address the increasingly diverse cyber threat environment, the New Mexico K-12 task force will implement a comprehensive cyber strategy to deter state and non-state actors from conducting malicious cyber activity against New Mexico K-12 and its interests.

The task force will invest in a framework to enable the New Mexico K-12 to work with public and private stakeholders to effectively respond to and mitigate the impact of cyber-attacks in New Mexico.

The specific goals outlined in this strategy represent the first step to realizing an improved cyber security posture across the State of New Mexico K12 community. This document identifies essential and achievable goals to enable and empower K12 entities across the State of New Mexico to improve their unique cyber security posture. Further, this strategy contains goals for improving cyber security education, training, and bolstering the cyber security workforce in New Mexico.

"Cyber threats are already challenging public trust and confidence in global institutions, governance, and norms, while imposing costs on the U.S. and global economies. Cyber threats also pose an increasing risk to public health, safety, and prosperity as cyber technologies are integrated with critical infrastructure in key sectors. The threats are amplified by our ongoing delegation of decision-making, sensing, and authentication roles to potentially vulnerable automated systems. This delegation increases the likely physical, economic, and psychological consequences of cyber-attacks and exploitation events when they do occur." Daniel R. Coats, Director of National Intelligence, 2017



Introduction

The inception of the New Mexico K12 task force stems from necessity at the District level to champion cyber security across the State of New Mexico. Announced as a joint memorial in 2020 – SJM 4 216534.1.

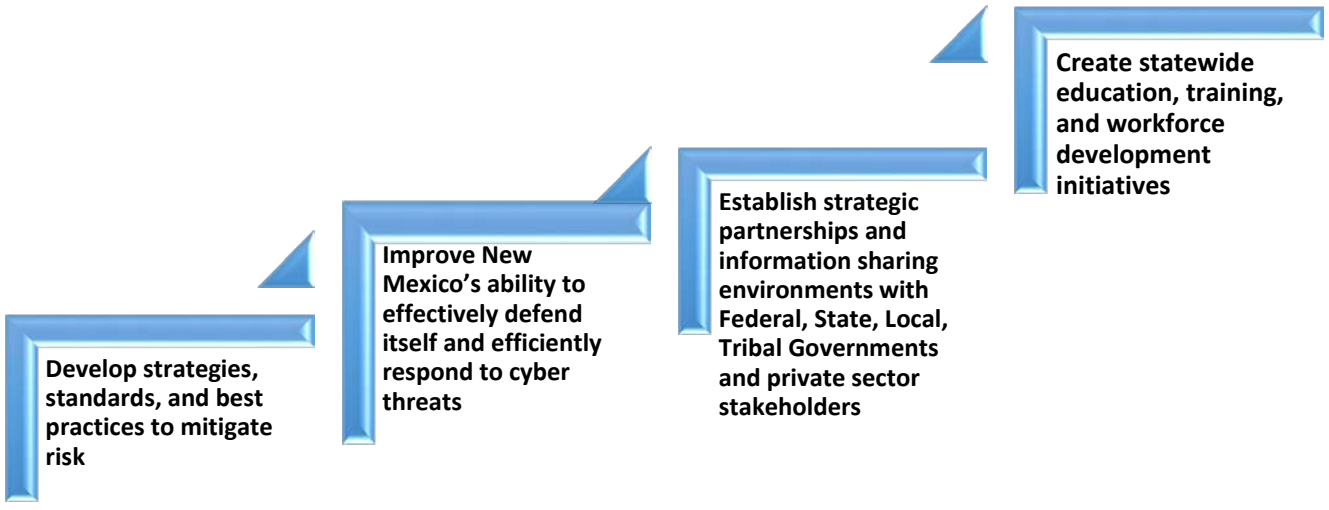
"At the end of the day, cyber security is not about technology, it's about managing risk." Brigadier General (retired) Gregory J. Touhill – the first Chief Information Security Officer (CISO) of the United States

The task force will work with state and partners for the synchronization and coordination of strategic cyber security initiatives within New Mexico. The task force will not replicate existing programmatic or budgetary mechanisms, or interfere with previously defined cyber security roles; rather, it will provide a single platform to integrate K12 cyber security initiatives, manage strategic policy and planning, and streamline cyber security governance structures. Further, the task force will provide advice and recommendations on key cyber issues to other K-12 entities along with the Governor's Office, New Mexico State Legislature, state agencies, political subdivisions and tribal governments.

Mission and Vision

K12TF Mission: Utilize new and existing resources, aided by the NM Higher Education community to augment local Districts and to help educate them with new strategies and tools to mitigate threats. To work in collaboration with the New Mexico PED and DoIT for Cyber Defense Coordination serves as the primary point for cyber security strategy, policy, planning, and coordination for the State of New Mexico.

K12TF Vision: To become a K12 leader in cyber security information management, by coordinating information, enabling effective risk management decisions, addressing cyber threats and advancing cyber security education and training. Key objectives include:



2020 – 2021 Strategic Goals

Strategic Goal 1: Adopt Information Management Policies, Guidance, and Best Practices

Current governance mechanisms require modernization and enhancement to meet the dynamic cyber threat landscape. As an example, recent data breaches across New Mexico highlight the need for improved governance structures and the elimination of silos. K12TF will develop methodologies to standardize cyber security practices by reviewing policies, regulations, emerging technologies, and best practices.

- **Goal 1.1:** The K12TF will develop a framework to complement existing business and cyber security operations in a holistic effort to identify, assess, and manage cyber security strategy and risk for K12 organizations in the State of New Mexico and its interests.
- **Goal 1.2:** Develop cyber security performance measurements to inform decision-making, highlight value, and ensure accountability.
    - As stewards of public funds, it is the responsibility of this group to establish clear and tangible cyber security objectives with measurable outcomes to the extent possible.
- **Goal 1.3:** Develop, in coordination with school districts', recommendations regarding State of New Mexico cyber security funding appropriations. Additionally, K12TF will ensure state investments are aligned to support a K12 whole-of-education approach to effective cyber security efforts.
- **Goal 1.4:** Craft or enhance continuity of operations plans and procedures to enable the State of New Mexico K12 to conduct business activities within a degraded or disrupted cyber environment, in the event of a successful cyber attack.
- **Goal 1.5:** K12TF will leverage private sector cyber security subject matter experts for input on trending cyber threats, best practices and guidance, and to perform unique ad hoc support and enhance the limited cyber security workforce, as necessary.

Strategic Goal 2: Safeguard Information Systems against Cyber Threats

Protection of New Mexico's K12 critical information resources is paramount to New Mexico's growing economy, health, and public safety. As part of this strategy, K12TF will work with key allies and partners to build networked cyber security capacity in an effort to secure critical infrastructure and key resources which New Mexico depends on for the continued delivery of essential services.

> *"The evolution of ransomware in 2017 should remind us of how aggressively a threat can reinvent itself as attackers dramatically innovate and adjust to the successful efforts of defenders," Steve Grobman, Chief Technology Officer, McAfee, LLC*

- **Goal 2.1:** K12TF will develop methodologies to efficiently evaluate New Mexico K12 information systems, in addition to associated policies, procedures, identified gaps, overlaps, conflicts, and areas in need of modernization. As part of this goal, K12TF will:
    - Assess the cyber security posture of individual state K12 Districts and associated strategies and assess the ability to deter bad actors from conducting successful cyber attacks against K12 and its interests.
- **Goal 2.2:** Understanding the wealth of unique state business operations/objectives, legal and regulatory requirements, and organizational constraints, K12TF will establish risk-based assessments of information systems operated and maintained by state agencies.
    - Through the K12 district assessment process of identification and prioritization, K12TF will develop strategies to mitigate identified security gaps and risk to critical and non-critical assets.
- **Goal 2.3:** Develop a cyber threat intelligence sharing platform to aid in situational awareness, risk management, system readiness, and identification of appropriate controls, as funding permits.
- **Goal 2.4:** Develop processes to accelerate notification of cyber security incidents to state and partner entities.

Strategic Goal 3: Develop Incident Response, Triage, and Recovery Teams

In an effort to address and respond to identified cyber attacks, K12TF will try to help mitigate the impact of cyber incidents through the creation of cyber response teams, with a focus to expand continuity of operations, reduce impact time, and increase resiliency. Cyber attacks are more dynamic than traditional threats and require timely response. Development of a response governance structure to adequately prepare and secure the State's K12 environment in an evolving threat landscape is paramount.

- **Goal 3.1:** Work to create cyber incident response teams with elements of the Department of Public Education and Department of Information Technology; additional team participation from federal, state, local, tribal governments and private-sector elements, as appropriate.
- **Goal 3.2:** Ensure recovery elements have clear understanding of organizational key assets, risk assessments, threat landscape, potential impact, and current controls in place to protect assets.

- **Goal 3.3:** Develop defined protocols and responsibilities for responding to cyber incidents/attacks.
- **Goal 3.4:** Develop and coordinate cyber security incident response training exercises with state and non-state partners to mature cyber response capabilities and readiness.

Strategic Goal 4: Foster Partnerships to Strengthen Cyber Ecosystem

The cyber ecosystem encompasses a variety of diverse contributors – federal, state, local, tribal government, and private-sector partners. Achieving a successful cyber security ecosystem relies, in part, on extensive and resilient partnerships that cultivate innovation, information sharing, and best practices.

K12TF will initiate a series of programs to create a healthy cyber ecosystem with a focus on collaboration in real-time to anticipate and prevent cyber-attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a normal environment.

- **Goal 4.1:** K12TF will develop a framework through integrated capabilities and robust partnerships with federal, state, local, tribal government, and private-sector entities to strengthen and defend New Mexico schools from cyber-attacks.
- **Goal 4.2:** To improve New Mexico's schools cyber defensive posture, K12TF will generate partnerships and strategies with schools to develop intelligence information sharing methodologies to disrupt or deter cyber-attacks before they impact New Mexico K12.
    - K12TF will further develop in partnerships for the management and exploitation of cyber threat information aggregated through information collaboration and relationships.
- **Goal 4.3:** To improve cyber threat situational awareness, K12TF will develop strategies to leverage continuous, automated, and standardized mechanisms for sharing critical information with stakeholders across the State of New Mexico.

Strategic Goal 5: Champion Cyber security Education and Training

To overcome the global cyber security skills shortage, New Mexico must rely on the development of an effective local cyber security workforce. K12TF will champion programs that help New Mexicans find the education and training they need to advance their careers to help reduce the skills gap in the field of cyber security. Specifically, K12TF will promote robust cyber security education, training, and workforce development initiatives through comprehensive partnerships in academia, local government, and private sector entities to cultivate a highly capable cyber workforce.

"Unfortunately the pipeline of security talent isn't where it needs to be to help curb the cybercrime epidemic. Until we can rectify the quality of education and training that our new cyber experts receive, we will continue to be outpaced by the Black Hats." Robert Herjavec, founder and CEO at Herjavec Group

- **Goal 5.1:** K12TF will help develop K12 cyber education initiatives in partnerships with New Mexico colleges and universities to aid in the development of a robust cyber workforce.
- **Goal 5.2:** Research long-term cyber workforce needs for New Mexico, and develop initiatives with government and not-for-profit workforce development agencies to encourage and strengthen advancement of cyber security careers.
- **Goal 5.3:** Create programs to inspire cyber security career awareness with students in elementary schools, stimulate cyber security career exploration in middle schools, and enable cyber security career preparedness in high schools.
- **Goal 5.4:** K12TF will raise awareness of the National Cyber Security Workforce Framework and encourage adoption.
- **Goal 5.5:** In collaboration with partner organization, K12TF will develop a training environment to conduct cyber attack exercises, experimentation, forensics, and assessment of cyber tactics, techniques, and procedures.

Conclusion

Legacy governance structures and policies will continue to prove ineffective in a dynamic cyber threat environment. Greater reliance on mobile devices, advances in artificial intelligence, expanded use of internet-of-things (IoT) connected devices, and the digital-physical world will further stress cyber security policy frameworks.

The development of a common language for internal and external communication of cyber security issues, efficient sharing of cyber threat information between stakeholders, improved situational awareness, and execution of best practices will be paramount for the successful strengthening of cyber security in New Mexico.

The goals outlined in this strategy represent the first step to realizing an improved cyber security posture across the NM K12 community. For the New Mexico K12TF to succeed in meeting these goals, leaders from across the state must take action to achieve the objectives outlined in this document. Additional resources, collaboration, execution, and accountability will prove vital for the success of these initiatives. The cyber threat environment can change rapidly. We must remain dynamic, adaptable, and tenacious to enhance and drive the cyber security paradigm forward.